bsi.

Standards at the Heart of Information Security

ISO/IEC 27001 Overview implementation guide

By Royal Charter

Enabling better business

Contents

Introduction

Information security standards

Information security is an essential part of any modern organization. Any size business, in any sector, will have some kind of data, information or assets that they will need to ensure are stored securely and accessible only by the right people at the right time.

Effective information security (infosec) requires a balance between risk management and technology, customers and stakeholders, staff and management. It can be challenging when faced with large amounts of different data, but with the right tools and information, organizations can protect commercially sensitive and personal data and keep their businesses safe.

What is ISO/IEC 27001?

ISO/IEC 27001 brings together knowledge and experience from the infosec industry, academia, the UK government and other sources to create a best practice guide to information security.

It's an approach that can be adopted by any business, either partially or in full, to improve how that organization keeps data safe. It offers best practice guidance on how to identify and respond to threats appropriately, how to make your business more resilient and robust to potential threats, and how to continually build on the learning to ensure you remain protected.

This guide will show you how you can implement ISO/IEC 27001 in your organization, either in part or full, to maximise the long-term benefits and safeguard your business.

Features and benefits

What can ISO/IEC 27001 do for your business?

The ability to manage information safely and securely has never been more important. ISO/IEC 27001 not only helps protect your business, but also sends a clear signal to customers, suppliers and the marketplace that your organization has the ability to handle information securely.

The benefits of ISO/IEC 27001

The benefits of ISO/IEC 27001 aren't just limited to information security, however. Adopting ISO/IEC 27001 could offer your business a range of benefits, by highlighting inefficiencies and processes that can be improved.

- Demonstrate your commitment to information security to marketing documents, branding and communications, making you more attractive to potential customers and allowing you to take on new work.
- Streamline and improve processes that may be outdated or simply ineffective. This could mean destroying existing data silos or coming up with completely new ways to do things.
- Save time by having effective processes in place, leaving more opportunities for innovation and focusing on the higher-value aspects of your business.

The benefits of ISO/IEC 27001 according to users:

Reduces business risk

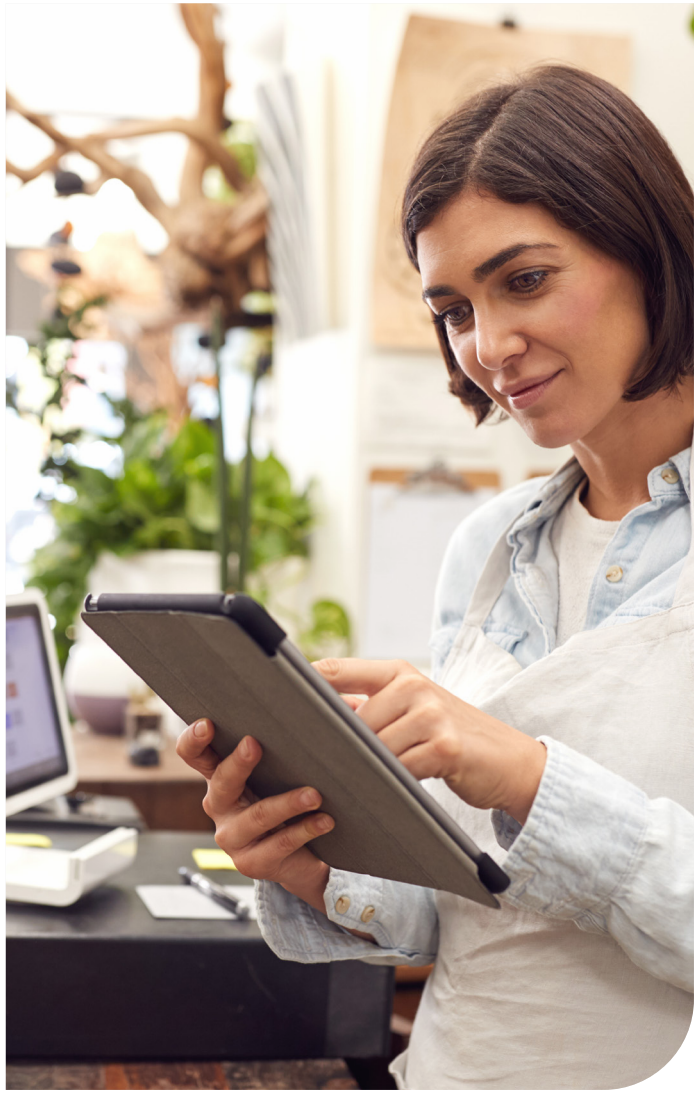
Inspires trust in our business

Helps protect our business

Helps us comply with regulations

Increases our competitive edge

Reduces the likelihood of mistakes



Core concepts: Learning the language of ISO/IEC 27001

Versions of ISO/IEC 27001

The latest version of ISO/IEC 27001 was published in 2013. ISO/IEC 27001:2013 was created to help face the challenges of modern business. It is backed up by the principles of risk management contained in ISO 31000. You can always find previous versions of a standard at BSI Knowledge, the online database of British Standards.

Key terminology:

Controls

Any administrative, managerial, technical or legal method used to modify or manage an information security risk, e.g. processes, policies, programs, tools or devices.

Risk owner

The person or entity with the authority to manage a particular risk and is accountable for doing so.

Documented information

The meaningful data or information you control or maintain to support your Information Security Management System (ISMS).

Interested parties

A person or entity that can affect, be affected by or perceive themselves to be affected by a decision or activity, e.g. suppliers, customers or competitors.

Issues

External or internal, positive or negative conditions that affect the confidentiality, integrity and availability of an organization's information.

Risks and opportunities

Defined as "the effect of uncertainty on an expected result".

Core concepts: Learning the language of ISO/IEC 27001

What does it involve?

ISO/IEC 27001 can help you identify vulnerabilities in your ISMS, with guidance on how to proactively control and manage any threats.

Before exploring the standard in more detail, it's valuable to get to grips with the core concepts that the standard is built around. These are the areas that ISO/IEC 27001 will help you to understand and focus on continually improving.

Context of the organization

This is a thread that runs throughout the standard and means understanding any internal and external factors and/or conditions that can affect your organization's information.

Understanding the context that your organization exists in will allow you to more clearly see any limitations - or opportunities - that the adoption of ISO/IEC 27001 may cause.

Risk

Naturally, ISO/IEC 27001 is highly focused on the identification, prevention and management of risk. Essentially, risk associated with threats (e.g. viruses, hackers targeting you) and opportunities (e.g. exploiting vulnerabilities in your ISMS) is best reduced by putting in place the best possible planning processes. This is a more effective course of action than preventive (or, reactive) action.

Leadership

Many of the standards' requirements are specific to top-level management, whether that's one person or a group of people. This may involve individuals at C-Suite, or working groups established to manage the adoption of the new standard, setting long- and short-term objectives, assigning tasks and setting deadlines.

Communication

This standard contains clear and detailed requirements for both internal and external communications at every level of the organization. For clients, customers, stakeholders or anyone else, changes being made as the standard is adopted must be communicated clearly and in good time.

Performance evaluation

A final but essential part of adopting any standard is how you'll measure the impact of adopting ISO/IEC 27001, analyse your ISMS and identify remaining areas for improvement. Whether you want to get certified or simply adopt some elements of the standard, evaluating and assessing your progress ensures you can keep building on what you've achieved.

Case study: Keeping data safe and secure with ISO/IEC 27001

As a company reliant on the safety and security of its customers' data, debt collection agency Fredrickson adopted ISO/IEC 27001 to demonstrate their commitment to information security. From building consumer confidence to saving time, the standard has resulted in a range of benefits for the organization, according to Sales and Marketing Director, Jan-Michael Lacy.

"Information security is fundamental to the success of Fredrickson. Much of our work involves receiving, analysing and storing sensitive consumer and business credit information. We must be able to assure our customers and the general public that we take the security of their personal information seriously.

Rather than simply saying that we are compliant with the information security standard BS ISO/IEC 27001, we felt it would provide the market with the confidence it needed if we got independent assessment and certification.

As a result, clients and the general public can now have total confidence in our information security practices and the way their personal information is managed.

Being able to show that we are BS ISO/IEC 27001 certified has significantly reduced the man hours needed to complete IT security questionnaires required by clients in bidding for work and on an ongoing basis after a contract has been awarded.

Introducing the standard also brought us immediate financial benefits. Since we achieved certification we have won some of our largest deals. Clients now include a central government department, well respected UK financial institutions and several FTSE 100 companies. We are committed to setting the standard and becoming the most compliant agency in the UK. We believe that in the near future BS ISO/IEC 27001 certification will be a pre-requisite imposed by many of our clients when selecting outsourced partners.

There have been several high profile instances of data loss within our industry and as such reducing the risk of this happening and proving we have the highest levels of security in place is important in demonstrating to clients that we are fit for purpose."

Jan-Michael Lacy
Sales and Marketing Director

"The standard isn't just for firms like ours – any business can benefit from it. Compliance also helps businesses to meet legal requirements such as data protection regulations and the Freedom of Information Act."

Your ISO/IEC 27001 journey

1. Discuss the possibility of adopting ISO/IEC 27001 with stakeholders, team leaders and staff to ensure it will add value to your organization and that everyone is on board with the implications of adoption – an ISO/IEC 27001 training session or external consultant can help with this.
2. Buy the standard and read it; understand the content, your requirements and how it will improve your business. Download your PDF version of the full standard and start exploring how you can enhance your information security.
3. Start planning your implementation strategy and reviewing existing processes as a benchmark to monitor progress against. Compare your current system with ISO/IEC 27001 approaches.
4. Create workgroups with defined roles, responsibilities and deadlines. These groups should be made up of different levels of staff, as they will use their practical experience to manage the adoption of the standard.
5. When you've fully implemented the standard, make sure you regularly review your ISO/IEC 27001 system to ensure continual improvement.
6. Encourage training opportunities that support your ISO/IEC 27001 system, such as staff becoming internal auditors.
7. Through BSI, or another third-party certification body, apply for full certification. Undertake the two-stage formal assessment which examines how you're applying the standard and checks procedures and controls in place are in line with ISO/IEC 27001.
8. Receive your ISO/IEC 27001 certification, which is valid for three years.

Understanding your standard

A breakdown of ISO/IEC 27001

The physical document that houses a standard is made up of clauses which guide you or your organization through the process of implementation. These clauses enable you to plan how you will adopt a standard like ISO/IEC 27001, from the very first step to post-certification.

To dispel the air of mystery around standards, we've broken down ISO/IEC 27001 into its separate clauses to explain how each one works, what it will require of your business and the intended outcome of each section.

Clause 1 and 2: Scope and references to other documents

The first clause details the scope of the standard. A lot of the documents referenced in ISO/IEC 27001 are contained in ISO/IEC 27000, such as:

- Information technology
- Security techniques
- Information security management systems
- Overview and vocabulary, which is referenced and provides valuable guidance

Clause 3 and 4: Terms and definitions and context of the organization

As with clause 2, refer to the terms and definitions contained in ISO/IEC 27000. Clause 4 establishes internal and external issues that may impact the implementation and effects of ISO/IEC 27001 on the ISMS.

This clause will talk you through identifying those issues, establishing your interested parties and any legal, regulatory or contractual obligations you may have to them. It'll then guide you through determining the scope of your ISMS and show you how to establish, implement, maintain and continually improve your ISMS in relation to ISO/IEC 27001.

Clause 5 and 6: Leadership and planning

Clause 5 focuses on the role of top management. While they can assign ISMS relevant responsibilities and authorities, they remain ultimately accountable for it, so they need to establish the ISMS and infosec policy, ensure those policies are clearly communicated to and understood by all parties and monitor the continual improvement of the ISMS.

Clause 6 outlines how you plan to address any of the risks and opportunities to information you have identified, focusing on how to deal with information security risks.

"Statement of Applicability" (SoA)

The SoA summarises your strategy around risk treatment, the control objectives and any controls you have included. It also details those you have excluded and explains why. The SoA establishes your infosec objectives clearly, concisely and in line with the standard's requirements.

Understanding your standard

Clause 7: Support

This section is about getting the right resources, people and infrastructure in place to establish, implement, maintain and continually improve your ISMS. From competence and communications to the availability of training and personnel, this clause focuses on documented information, how you'll protect it and who has access to it.

Clause 8: Operation

By clause 8, you're ready to execute the plans and processes you've come up with. This clause is where you can start working towards achieving your infosec objectives in a controlled way.

Consider any changes - whether planned or not - and record and retain the results of any new process being implemented.

Clause 9: Performance evaluation

Monitoring, measuring, analyzing and evaluating your ISMS ensures that it is effective and will remain so. Clause 9 guides you through continually assessing your organization, from considering how you'll evaluate your infosec's effectiveness to anaylzing the methods you used. This is where internal audits and management reviews will take place and you can identify areas for improvement.

Clause 10: Improvement

The last clause is a chance to identify any corrective action that might be needed. Clause 10 requires you to:

- Show how you react to nonconformities, take action, correct them and deal with the consequences.
- Demonstrate whether any similar nonconformities exist, or could happen, and show how you'll eliminate their causes
- Show continual improvement of the ISMS, including demonstrating the suitability and adequacy of it and how effective it is. However, how you do this is up to you

BSI's implementation top tips

1. Explore the best practice advice within the standard and decide whether you wish to adopt in full and reach certification or just use the valuable information to improve your internal systems.
2. Think about how different departments work together to avoid silos. Make sure the organization works as a team for the benefit of customers and the organization.
3. Top management commitment is key to making implementation of ISO/IEC 27001 a success. They need to be actively involved and approve the resources required.
4. Review systems, policies, procedures and processes you have in place – you may already do much of what's in the standard, and make it work for your business. You shouldn't be doing something just for the sake of the standard – it needs to add value.
5. Speak to your customers and suppliers. They may be able to suggest improvements and give feedback on your service.
6. Train your staff to carry out internal audits of the system. This can help with their understanding, but it could also provide valuable feedback on potential problems or opportunities for achievement.
7. When you gain certification celebrate your achievement and use the BSI Assurance Mark on your literature, website and promotional material.

Start your standards journey

Visit BSI Knowledge to explore over 60,000 standards. For more information about ISO/IEC 27001 contact our customer service team on 0345 086 9001.

+44(0)345 086 9001
bsigroup.com